AMENDMENTS TO THE DRAWINGS

Proposed drawing changes are shown on the attached annotated marked up drawing and are incorporated within an attached proposed replacement sheets of drawings.

Attachment: Replacement Sheet(s)
Annotated Sheet Showing Changes

REMARKS/ARGUMENTS

Reconsideration of this application is respectfully requested.

In response to the Examiner's formality-based objections to the drawings, specification and claims, the above amendments to the drawings, specification and claims are believed to obviate all outstanding formality-based grounds of objection/rejection. If any remaining formal issues are believed to be present, it is respectfully requested that the undersigned be telephoned so that they may be obviated efficiently.

The rejection of claims 1, 2, 5-6, 21, 22 and 25-43 under 35 U.S.C. §102 as allegedly being anticipated by Perrig is respectfully traversed.

The present invention and Perrig are both concerned with methods for managing a cryptographic key group comprising a large set of users when the membership in the group changes i.e. when members leave or join the group.

In both cases, using Figure 1 of the present application as an example, the binary tree depicts a group with three members M1, M2 and M3 who share a root node K14. K14 can be used to encrypt transmissions sent to the members so that parties outside the group who do not have the key K14 cannot access the transmission so encrypted. The intermediate nodes K1, K2 and so on are also cryptographic keys, each of which enable the member to access the root key K14. Please see applicant's specification at page 14 line 33 to page 15 line 10.

When a leave or join event occurs, resulting in a change in the membership of the group, the root key K14 has to be changed, to prevent an ex-member who already knows K14 from accessing new secure group transmissions, and to prevent a new member from accessing information which had been previously encrypted using K14. Hence in Figures 2 and 3 which respectively depict a join event (new member M4) and a leave event (member M3 had left) root

key K14 is replaced respectively by new keys K14' and K14" by the key server. The members of the changed groups need to be provided information to enable them to access the new keys K14' and K14", as the case may be. Please see applicant's specification at page 3 line 29 to page 5 line 28.

As explained on page 9 line 33 to page 10 line 3 of the applicant's specification key access information is typically broadcast in an encrypted form to prevent parties outside the group from accessing the information. This is the method used in Perrig: e.g. page 7 right-hand column paragraph 5 "the key server sends the new member all updated keys on its key path ... over a secure channel".

This is one of the areas where the presently claimed invention differs from Perrig. Key update information in applicant's invention can be broadcast without need for encryption (see page 29 line 14 and 15; page 30 lines 9 to 11). This is achieved by use of "offset messages to implement the key update and key recovery mechanisms", where an "offset message can be considered to be the distance between two chains of one-way functions" (page 12 lines 24 to 28). Figure 4 illustrates the process described on page 12 lines 28 onwards. Referring now to both Figures 3 and 4, assume key Y1 of Figure 4 to be node K1 on the tree of Figure 3, and key X2 to be the node K12 on the tree of Figure 3. If key Y1/K1 is known, then X2/K12 can be generated using the formula on page 13 lines 9 to 21 if the correct offset message is also known to Y1/K1.

To ensure the security of a key update message, the key server generates intermediate keys as described on page 14 lines 4 to 25.

In short, one way the presently claimed invention differs from Perrig in that, for example, the applicant's key update messages need not be encrypted for broadcast, due to the use of offset

messages. The use of double functions as depicted in Figure 5 ensures security even without encryption.

Claim 1 covers a method of using an offset "for generating the updated first key of each node ...", and claim 2 includes the further feature of using two one-way functions and a mixing function which includes the offset as a parameter of the mixing function.

Perrig does not use anything like an offset to enable generation of keys, but instead conventionally broadcasts a secure (i.e. encrypted) key update message.

In addition to the fact that each of applicant's independent claims requires a novel "offset" not taught or suggested by Perrig, the pending claims have been above amended so as to now also require the offset value to be broadcast in an unencrypted form. This, of course, even further emphasizes this particular point of distinction from Perrig.

Since anticipation requires the allegedly anticipating reference to teach each and every limitation of the rejected claims, it is believed sufficient to have now noted one of the important distinctions between applicants claimed invention and Perrig *vis-a-vis* the rejected claims.

The rejection of claims 3, 4, 23, 24, 44 and 45 under 35 U.S.C. §103 as allegedly being made "obvious" based on Perrig in view of Dondeti '188 is also respectfully traversed.

Fundamental deficiencies of Perrig have already been noted above with respect to parent claims. Dondeti does not supply those deficiencies.

Accordingly, it is not believed necessary at this time to detail the additional deficiencies of this allegedly "obvious" combination of references with respect to these rejected claims.

The rejection of claims 17-20 under 35 U.S.C. §103 as allegedly be made "obvious" based on Perrig in view of Bright '497 is also respectfully traversed.

Once again, the fundamental deficiencies of Perrig have already been noted with respect to a parent claim. Bright does not teach those deficiencies.

Accordingly, it is not believed necessary at this time to explain the further deficiencies of this allegedly "obvious" combination of references with respect to these rejected claims.

Accordingly, this entire application is now believed to be in allowable condition and a formal notice to that effect is respectfully solicited.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: Larry S. Nixon
Larry S. Nixon
Reg. No. 25,640

LSN:tlm
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100

Fig.1.
(PRIOR ART)

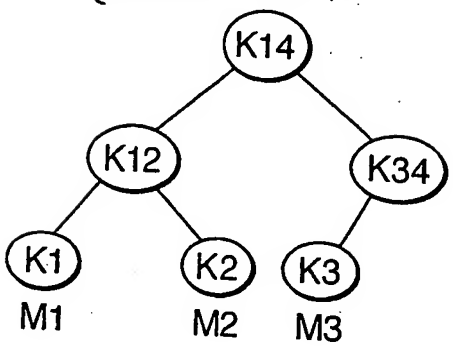
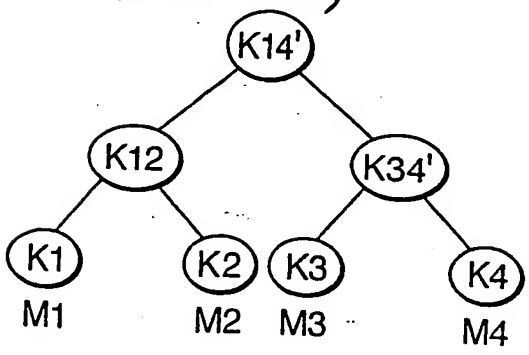


Fig.2.
(PRIOR ART)



ANNOTATED MARKED UP DRAWINGS
FOR SN 10/507,114

Fig.3.
(PRIOR ART)

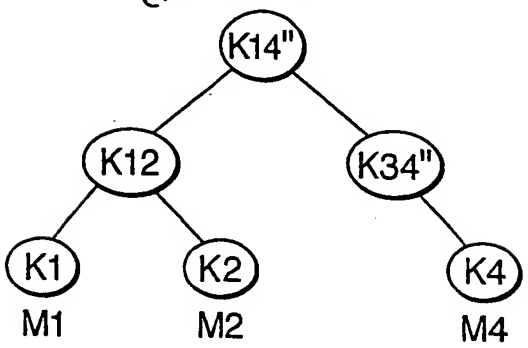


Fig.4.